

REMARKS

This Amendment is in response to the Office Action mailed July 26, 2007. In the Office Action, claim 13 was rejected under 35 U.S.C. §112 (second paragraph) and claims 13-19 were rejected under 35 U.S.C. §103. Claims 1-12 have been cancelled without prejudice. Claims 13 and 17 have been amended. Claims 20-22 have been added.

Reconsideration in light of the amendments and remarks made herein is respectfully requested.

Request for Examiner's Interview

Applicant respectfully requests the Examiner to contact the undersigned attorney to discuss the allowability of the pending claims especially if, after his review, there are still questions regarding patentability. The undersigned attorney can be reached at the telephone number listed below.

Rejection Under 35 U.S.C. § 112

Claim 13 was rejected under 35 U.S.C. § 112, second paragraph, as being allegedly indefinite. Applicant has amended claim 13 to remove the term "substantially". Hence, Applicant respectfully requests that the Examiner withdraw the rejection of claim 13 under 35 U.S.C. § 112, second paragraph.

Rejection Under 35 U.S.C. § 103

Claims 13-19 were rejected under 35 U.S.C. §103(a) as being unpatentable over Proudler (U.S. Publication No. 2003/0226031) in view of Clapp (U.S. Patent No. 5,987,131) and Ober (U.S. Patent No. 6,959,086). Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established.

As the Examiner is aware, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify a reference or to combine reference teachings. Second, there must be a reasonable expectation of

success. Finally, the prior art reference (or references when combined) must teach or suggest all of the claim limitations. *See MPEP §2143; see also In Re Fine, 873 F. 2d 1071, 5 U.S.P.Q.2D 1596 (Fed. Cir. 1988).* Herein, the combined teachings of the cited references fail to describe or suggest all of the claim limitations.

For instance, with respect to claim 13, Applicant respectfully submits that none of the cited references, alone or in combination, describe or suggest the operation of proving in a single direct proof that a value was signed by a signature key without revealing the value. The term "direct proof" has been defined in the claims. Moreover, Applicant has added a limitation associated with the exponentiations, namely each of the plurality of exponentiations is of the form " $h^t \bmod P$," where h is a unique number, t is randomly chosen number (e.g., $0 \leq t \leq W$, where $W \geq 280$) and P is a prime number. The same argument is applicable to the system claim set forth in claim 17.

Applicant respectfully requests that the Examiner withdraw the rejection of claims 13-19 under 35 U.S.C. §103(a).

Conclusion

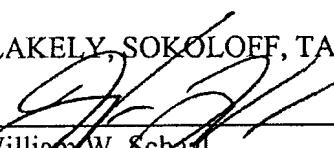
Applicant respectfully requests that the Examiner reconsider the rejections and issue a timely Notice of Allowance.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: October 26, 2007

By


William W. Schaal

Reg. No. 39,018

Tel.: (714) 557-3800 (Pacific Coast)